

DEVICE AND METHOD FOR CONTROLLING PROGRAM AND PROGRAM

Publication number: JP2002351567 (A)

Publication date: 2002-12-06

Inventor(s): NANA O SHINJI; TAKEUCHI TAKASHI;
ICHIHARA NAOHISA; YAMAMOTO SHINYA

Applicant(s): NTT DATA CORP

Classification:

- international: **B42D15/10; G06F1/00; G06F21/22;
G06K19/073; B42D15/10; G06F1/00;
G06F21/22; G06K19/073; (IPC1-7): G06F1/00;
B42D15/10; G06K19/073**

- European:

Application number: JP20010159183 20010528

Priority number(s): JP20010159183 20010528

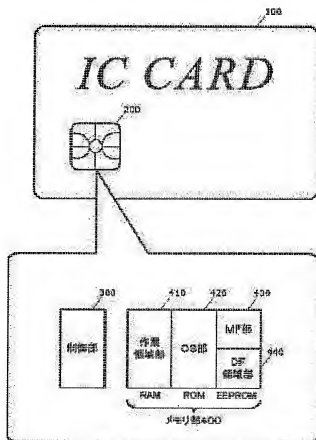
Also published as:

JP4028697 (B2)

Abstract of JP 2002351567 (A)

PROBLEM TO BE SOLVED: To provide a program controller and a program controlling method capable of effectively establishing security in carrying out a program and to provide a program.

SOLUTION: A controlling part 300 in an IC chip 200 mounted on an IC card 100 performs a security program recorded in an OS part 420 when initialized. In a DF area part 440, a plurality of kinds of programs for realizing a plurality of kinds of services are recorded in a plurality of areas. When an area corresponding to a desired service is designated, the controlling part 300 sets a hardware firewall (HFW) in the corresponding area on the basis of the operation of the security program. The HFW inhibits designation of another service during the performance of the program of the designated service and inhibits the program in execution from performing a program of another service.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-351567

(P2002-351567A)

(43) 公開日 平成14年12月6日 (2002.12.6)

(51) Int.Cl.

識別記号

F I

データ(参考)

G 0 6 F 1/00

B 4 2 D 15/10

5 2 1

2 C 0 0 3

B 4 2 D 15/10

G 0 6 F 9/06

6 6 0 C

5 B 0 3 3

G 0 6 K 19/073

C 0 6 K 19/00

P

5 B 0 7 6

審査請求 有 請求項の数9 O L (全10頁)

(21) 出願番号 特願2001-159183(P2001-159183)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目3番3号

(22) 出願日 平成13年5月28日(2001.5.28)

(72) 発明者 七尾 慎司

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(72) 発明者 竹内 隆

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(74) 代理人 100095407

弁理士 木村 満

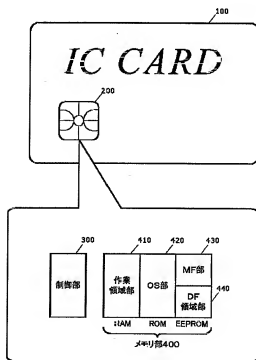
最終頁に続く

(54) 【発明の名称】 プログラム制御装置および方法、ならびにプログラム

(57) 【要約】

【課題】 プログラム実行時の安全性を効果的に確立することができるプログラム制御装置および方法、ならびにプログラムを提供することを目的とする。

【解決手段】 ICカード100に実装されているICチップ200内の制御部300は、イニシャライズ時にOS部420に記録されているセキュリティプログラムを実行する。DF領域部440には、複数種類のサービスを実現するための複数種類のプログラムが複数の領域に記録されている。所望のサービスに対応する領域が指定されると、セキュリティプログラムの動作に基づいて、制御部300は当該領域に対してハードウェアファイアウォール(HFW)を設定する。HFWにより、指定されたサービスのプログラム実行中は、他のサービスのプログラムを実行することが禁止される。



【特許請求の範囲】

【請求項1】複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御装置であり、

所定のサービスを実現するための少なくとも1つのプログラムを、前記複数の記憶領域のいずれか1つに割り当て

るプログラム割当手段と、

実行するサービスを指定するサービス指定手段と、

前記サービス指定手段が指定したサービスを実現するプログラムを実行するプログラム実行手段と、

前記サービス指定手段がサービスを指定したことを契機に、前記サービス指定手段および前記プログラム実行手段を制御し、前記プログラム実行手段が同時に実行できるプログラムを、前記サービス指定手段が指定したサービスに対応するプログラムが割り当てられた記憶領域に記録されているプログラムに制限する実行制限手段と、

を備える、ことを特徴とするプログラム制御装置。

【請求項2】前記サービス指定手段は、指定したサービスに対応する記憶領域内のディレクトリを指定し、前記実行制限手段は、前記サービス指定手段が指定したディレクトリに属するプログラムのみが実行されるよう、前記プログラム実行手段を制御する、ことを特徴とする請求項1に記載のプログラム制御装置。

【請求項3】前記実行制限手段は、前記プログラム実行手段がプログラムを実行している間、前記サービス指定手段が他のサービスを指定することを禁止する指定制限手段と、前記プログラム実行手段が実行しているプログラムが他の記憶領域へのアクセスを要求しても、前記プログラム実行手段が他の記憶領域へアクセスすることを禁止するアクセス制限手段と、を備える、ことを特徴とする請求項1または2に記載のプログラム制御装置。

【請求項4】前記記憶媒体はICカードのプログラム記憶領域であり、前記プログラム制御装置は前記ICカードに実装されている、ことを特徴とする請求項1乃至3のいずれか1項に記載のプログラム制御装置。

【請求項5】複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御方法であり、

所定のサービスを実現するための少なくとも1つのプログラムを、前記複数の記憶領域のいずれか1つに割り当てるプログラム割当ステップと、

実行するサービスを指定するサービス指定ステップと、前記サービス指定ステップで指定されたサービスを実現するためのプログラムを実行するプログラム実行ステップと、

前記サービス指定ステップでサービスが指定されたことを契機に、前記プログラム実行ステップで同時に実行されるプログラムを、前記サービス指定ステップで指定されたサービスに対応する記憶領域に記録されているプログラムに制限する実行制限ステップと、

を備える、ことを特徴とするプログラム制御方法。

【請求項6】前記サービス指定ステップでは、指定したサービスに対応するプログラムが割り当てられている記憶領域内のディレクトリが指定され、

前記実行制限ステップは、前記プログラム実行ステップで実行されるプログラムが、前記サービス指定ステップで指定されたディレクトリに属するプログラムのみとなるよう制限する、

ことを特徴とする請求項5に記載のプログラム制御方法。

【請求項7】前記実行制限ステップは、前記プログラム実行ステップでプログラムが実行されている間、前記サービス指定ステップによる他のサービスの指定を禁止する指定制限ステップと、前記プログラム実行ステップで実行されているプログラムが、他の記憶領域へのアクセスを要求しても、該他の記憶領域がアクセスされることを禁止するアクセス制限ステップと、を備える、ことを特徴とする請求項5または6に記載のプログラム制御方法。

【請求項8】前記記憶媒体はICカードのプログラム記憶領域であることを特徴とする請求項5乃至7のいずれか1項に記載のプログラム制御方法。

【請求項9】コンピュータを、請求項1乃至4のいずれか1項に記載のプログラム制御装置として機能させるプログラム。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】本発明は、プログラム制御装置および方法、ならびにプログラムに関し、特に、ICカードに記録されたプログラムの実行に好適なプログラム制御装置および方法、ならびにプログラムに関する。

【0002】

【従来の技術】集積回路(ICチップ(IC: Integrated Circuit))を実装したICカード(スマートカード)が普及しつつある。ICカードは集積回路を実装しているため、従来の磁気カードなどに比べて記憶容量が圧倒的に大きいことに加え、自らプログラムを実行することができるので、広範囲な利用用途が期待されている。特に、複数のアプリケーションプログラムを記録し、それぞれをICカード自身で実行することができるので、1枚のICカードで複数種類のサービスの利用が可能となる、いわゆるマルチアプリケーション(マルチサービス)の用途に有用である。

【0003】つまり、1枚のICカードを、IDカード、クレジットカード、キャッシュカード、電子財布

(電子マネー)、各種会員カード、ポイントカード、電子キー、電子チケット、などといった種々の用途に用いることができる。このような複数種類のサービス利用を実現するため、ICカードには通常、使用者の用途に応じたアプリケーションプログラムを動的に記録・更新できる機能が備えられている。アプリケーションプログラムを動的に記録・更新できることで、使用者は所望する用途に応じたサービスの利用ができる反面、不正なプログラムを記録・実行することによる不正使用の可能性も高くなる。

【0004】このような問題に対処するため、ICカードにハードウェアファイアウォール (Hardware Firewall、以下「HFWF」と称す) を実装したものも存在する。このHFWFは、各プログラムがアクセスできるメモリ領域を制限することで、他のサービスにかかるプログラムやデータの実行、読み出し、書き込みを制御し、不正実行を防止する。

【0005】しかし、従来のHFWFの場合、制限されたメモリ領域にプログラムがアクセスしていないかを常に監視する必要があるため、各プログラムを常に実行可能な状態にしておく必要があった。このため、あるプログラム内に他のプログラムへジャンプするコマンド存在しそれが実行された場合、すべてのプログラムが実行可能な状態にあるため、他のプログラムへのジャンプが実行され、不正使用がなされてしまう可能性があった。

【0006】また、アクセスを制限するメモリ領域をプログラム毎に予め設定 (固定的に設定) する必要があるため、一度設定した後に、新たなアプリケーションプログラムを記録した場合、そのプログラムに対してはファイアウォールは有効とはならない。このため、追加・更新したプログラムに対して安全性を確立することができず、複数種類のプログラムを記録することで種々のサービスが利用できるICカードの利点を阻害してしまうという問題があった。

【0007】

【発明が解決しようとする課題】本発明は、上記状況に鑑みてなされたもので、プログラム実行時の安全性を効果的に確立することができるプログラム制御装置および方法、ならびにプログラムを提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するため、本発明の第1の観点にかかるプログラム制御装置は、複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御装置であり、所定のサービスを実現するための少なくとも1つのプログラムを、前記複数の記憶領域のいずれか1つに割り当てるプログラム割当手段と、実行するサービスを指定するサービス指定手段と、前記サービス指定手段が指定したサービスを実現するプログラムを実行

するプログラム実行手段と、前記サービス指定手段がサービスを指定したことを契機に、前記サービス指定手段および前記プログラム実行手段を制御し、前記プログラム実行手段が同時に実行できるプログラムを、前記サービス指定手段が指定したサービスに対応するプログラムが割り当てられた記憶領域に記録されているプログラムに制限する実行制限手段と、を備える、ことを特徴とする。

【0009】上記プログラム制御装置において、前記サービス指定手段は、指定したサービスに対応する記憶領域内のディレクトリを指定し、前記実行制限手段は、前記サービス指定手段が指定したディレクトリに属するプログラムのみが実行されるよう、前記プログラム実行手段を制御することが望ましい。

【0010】上記プログラム制御装置において、前記実行制限手段は、前記プログラム実行手段がプログラムを実行している間、前記サービス指定手段が他のサービスを指定することを禁止する指定制限手段と、前記プログラム実行手段が実行しているプログラムが他の記憶領域へのアクセスを要求しても、前記プログラム実行手段が他の記憶領域へアクセスすることを禁止するアクセス制限手段と、を備えることが望ましい。

【0011】上記プログラム制御装置において、前記記憶媒体はICカードのプログラム記憶領域であり、前記プログラム制御装置は前記ICカードに実装されているものとすることができる。

【0012】上記のような構成によれば、例えば、ICカードなどの記録媒体に複数種類のサービスを実現するための複数種類のプログラムが記憶されている場合、例えば、サービスを利用するためのホスト端末などからの指示に基づいて、ICカードが実現できるサービスのいずれかが指定されたことを契機に、実行可能なプログラムが、指定されたサービスに割り当てられた記憶領域内のプログラムに制限される。つまり、サービスの指定を契機に (動的に)、対象記憶領域にいづゆるハードウェアファイアウォール (HFWF) が設定される。これにより、予めHFWFを固定的に設定する場合と異なり、常にすべてのプログラムを実行可能な状態にしておく必要がない。このため、実行中のプログラムが他のサービスのプログラムを実行してしまう事態を防止することができ、プログラム実行時の安全性を向上させることができる。さらに、予め制限対象のメモリ領域を設定しておく必要がないので、アプリケーションプログラムをインストールする記憶領域の自由度を高くすることができ、インストールするプログラムの数や容量に柔軟に対応することができる。

【0013】この場合、例えば、指定された記憶領域にディレクトリが設定されている場合、サービス指定手段は、所望するプログラムを直下を含んだディレクトリを指定し、実行制御手段は、指定されたディレクトリ直下

のプログラムのみが実行されるよう、プログラム実行手段を制御する。これにより、所定のサービスを実現するためのプログラムのみが実行される。

【0014】さらに、サービスの指定を契機に設定されたHWWFにより、所定のサービスのためのプログラムが実行されている間、サービス指定手段が他のサービスを指定することを禁止する。また、実行中のプログラムが、他のサービスにかかるプログラムの実行を要求しても、その実行は禁止される。これにより、所定のサービスにかかるプログラムのみが実行されるので、プログラム実行時の安全性を向上させることができる。

【0015】上記目的を達成するため、本発明の第2の観点にかかるプログラム制御方法は、複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御方法であり、所定のサービスを実現するための少なくとも1つのプログラムを、前記複数の記憶領域のいずれか1つに割り当てたプログラム割当ステップと、実行するサービスを指定するサービス指定ステップと、前記サービス指定ステップで指定されたサービスを実現するためのプログラムを実行するプログラム実行ステップと、前記サービス指定ステップでサービスが指定されたことを契機に、前記プログラム実行ステップで同時に実行されるプログラムを、前記サービス指定ステップで指定されたサービスに対応する記憶領域に記録されているプログラムに制限する実行制限ステップと、を備える、ことを特徴とする。

【0016】上記プログラム制御方法において、前記サービス指定ステップでは、指定したサービスに対応するプログラムが割り当てられている記憶領域内のディレクトリが指定され、前記実行制限ステップは、前記プログラム実行ステップで実行されるプログラムが、前記サービス指定ステップで指定されたディレクトリに属するプログラムのみとなるよう制限することが望ましい。

【0017】上記プログラム制御方法において、前記実行制限ステップは、前記プログラム実行ステップでプログラムが実行されている間、前記サービス指定ステップによる他のサービスの指定を禁止する指定制限ステップと、前記プログラム実行ステップで実行されているプログラムが、他の記憶領域へのアクセスを要求しても、該他の記憶領域がアクセスされることを禁止するアクセス制限ステップと、を備えることが望ましい。

【0018】上記プログラム制御方法において、前記記憶領域はICカードのプログラム記憶領域であるものとすることができる。

【0019】上記目的を達成するため、本発明の第3の観点にかかるプログラムは、コンピュータを、上記プログラム制御装置として機能させることを特徴とする。

【0020】

【発明の実施の形態】以下、図面を参照して本発明にかかる実施の形態を説明する。

【0021】図1は本発明の実施の形態にかかるICカード（スマートカード）の構成を説明するための図である。図示するようにICカード100には、ICチップ200が実装されている。同図下段は、ICチップ200の構成を模式的に示している。図示するように、ICチップ200は、制御部300およびメモリ部400を備えている。メモリ部400はさらに、作業領域部410、OS部420、MF部430およびDF領域部440を備えている。

【0022】制御部300は、例えば、CPU（Central Processing Unit：中央演算処理装置）などから構成され、ICカード100を利用するためのホスト端末（不図示）からの指示（コマンド）に基づいてメモリ部400を制御し、プログラムおよびデータの読み出し、書き込みおよび実行を行う。

【0023】作業領域部410は、例えばRAM（Random Access Memory）などの読み書き可能な半導体記憶装置から構成され、制御部300がプログラムを実行する際のワークエリアとして用いられる。

【0024】OS（Operating System：基本ソフトウェア）部420は、例えばROM（Read Only Memory）などの読み出し専用の半導体記憶装置から構成され、制御部300が動作するための基本ソフトウェア（OS）などを記憶する。制御部300は、OS部420に記録されているOSを実行することにより、ICカード100の各部を制御し、後述する各処理を実現する。

【0025】また、このOS部420には、制御部300が後述するDF領域部440に記録されているアプリケーションプログラムを実行する際のセキュリティ動作を行うセキュリティプログラムが記録されているものとする。本実施の形態にかかるハードウェアファアウォール（HWWF）機能（後述）の動作は、制御部300がセキュリティプログラムを実行することで実現される。

【0026】このOS部420に記録される各プログラムは、ICチップ200の製造時に記録されるものである。

【0027】MF（Master File：マスタファイル）部430は、例えばEEPROM（Electrically Erasable Programmable Read-Only Memory）などの書換可能な不揮発性半導体記憶装置から構成され、後述するDF領域部440の根幹となるディレクトリ（以下、「MFディレクトリ」と称す）が作成される。このMFディレクトリは、ICカード100がイニシャライズされた場合のカレントディレクトリとして設定されるものである。

【0028】また、MF部430のMFディレクトリ直下には、後述するDF領域部440に記録されている各プログラム（アプリケーションプログラム）が共通に実行可能な共通プログラムが格納されている。この共通プログラムは、動的に追加・更新可能（ダウロード可

能)であり、MFディレクトリ直下に共通プログラムがダウンロードされた場合には、DF領域部440内の各アプリケーションプログラムによる実行が可能となる。

【0029】なお、本実施の形態では、OS部420に記録されているセキュリティプログラムのサブプログラムが共通プログラムとしてMF部430に記録されるものとする。これは、セキュリティプログラムはICカード100の初回使用時から実行されるべき重要なプログラムであるため、ICカード100の発行時(より詳細にはICチップ200の製造時)にOS部420に記録されるが、カード発行後にセキュリティプログラムの脆弱性が判明する場合がある。これに対処するため、追加・更新可能なMF部430に、セキュリティプログラムのサブプログラムやデータを動的に記録(ダウンロード)するようにし、常に最新のセキュリティ環境を実現できるようにする。つまり、後述するHWWFの動作では、OS部420のセキュリティプログラムとMF部430のサブプログラムとの協働により実現されるものである。

【0030】DF(Dedicated File:専用ファイル)領域部440は、例えばEEPROM(Electrically Erasable Programmable Read-Only Memory)などの書換可能な不揮発性半導体記憶装置から構成され、ICカード100を利用した複数種類のサービスを実現するためのプログラム(アプリケーションプログラム)やデータが格納される。DF領域部440はさらに、図2に示すようにサービス毎に記憶領域が分割される。本実施の形態では、ICカード100で利用できるサービスをサービス1～サービスn(例えば、サービス1は「電子財布」、サービス2は「IDカード」、サービスnは「電子キー」とする)とし、DF領域部440は、各サービスに対応したサービス別領域440-1～440-nを有するものとする。

【0031】図3は、MF部430とDF領域部440との関係を模式的に示した図である。図示するように、DF領域部440の各サービス別領域440-1～440-nには、それぞれのサービスに必要となるプログラムファイル、データファイルなどが格納されている。また、各サービス別領域440-1～440-nには、必要に応じてさらにディレクトリが用意され、それぞれのディレクトリにプログラムファイルやデータファイルが格納されている。

【0032】次に、図4のフローチャートを参照して、本実施の形態にかかるICカード100のプログラム実行処理を説明する。

【0033】まず、ICカード100が、所望するサービスを提供するホスト端末(不図示)に装着されるなどして、ICカード100とホスト端末との交信が開始されると(ステップS101:Yes)、ホスト端末はICカード100に対しインチャイス用のコマンドを発

行する。

【0034】ICカード100の制御部300は、ホスト端末からインチャイス用コマンドを受信すると、OS部420のOSおよびセキュリティプログラムが実行される(ステップS102)。

【0035】ステップS102で実行されたOSの動作に基づいて、制御部300は、図5(a)に示すように、MF部430のMFディレクトリをカレントディレクトリとして設定する(ステップS103)。MFディレクトリがカレントディレクトリとなることで、MFディレクトリ直下の共通プログラム、つまり、セキュリティサブプログラムが実行可能状態となる。このセキュリティサブプログラムは、ステップS102で起動されたセキュリティプログラムの指示により実行されるものとする。なお、図5、6、8において、実行中あるいは実行可能状態のプログラムを反転表示にて示すものとする。

【0036】次に、ホスト端末から、当該ホスト端末が提供するサービスを指定するコマンドがICカード100に送信されると(ステップS104:Yes)、制御部300は、当該サービスに対応するサービス別領域440-1～440-nのルートディレクトリをカレントディレクトリに設定する(ステップS105)。ここでは、サービス1が指定された場合を例に説明する。

【0037】ステップS102およびS103で起動されたセキュリティプログラムの動作に基づいて、制御部300は、ステップS105でルートディレクトリをカレントディレクトリに設定したことを契機に、当該ルートディレクトリに対応するサービス別領域440-1にハードウェアファイアウォール(Hardware Firewall、以下「HWWF」と称す)を設定する(ステップS106、図5(b))。つまり、HWWFを動的に設定する。ここで、サービス1のルートディレクトリの下にはディレクトリが存在していないため(ステップS107:No)、同図にて反転表示で示すように、ルートディレクトリ直下のプログラムが実行可能状態となる。つまり、カレントディレクトリの直下に存在するプログラムのみが実行可能状態となる(ステップS109)。

【0038】一方、サービス別領域440-1～440-n内に、複数のディレクトリが存在する場合(サービス2の例)は、セキュリティプログラムの動作に基づいて、サービス2の指定、つまりルートディレクトリが指定されたこと(ステップS105)を契機に、制御部300はサービス2に対応するサービス別領域440-2にHWWFを設定する(ステップS106、図6(a))。

【0039】ホスト端末が、必要なプログラムが格納されているディレクトリ(同図中ディレクトリ1)を指定すると(ステップS107:Yes)、図6(b)にて反転表示で示すように、ディレクトリ1直下のプログラ

ムが実行可能状態となる。つまり、カレントディレクトリの直下に属するプログラムのみが実行可能状態となる。

【0040】そして、制御部300が、実行可能状態となったプログラムを実行する。つまり、ステップS107にてディレクトリの指定があった場合には(ステップS107:Yes)、当該ディレクトリ直下のプログラムが実行され(ステップS108)、ルートディレクトリ以外のディレクトリが存在しないサービスが選択された場合(ステップS107:No)は、ルートディレクトリ直下のプログラムが実行される(ステップS109)。

【0041】ステップS108またはS109にてプログラムが実行されると、ステップS106で設定されたHWWFにより、実行されているプログラムの動作が監視される(ステップS200)。

【0042】このHWWFによるプログラム監視処理を、図7のフローチャートを参照して説明する。ここでは、図6(b)に示すように、サービス別領域440-2(サービス2)のディレクトリ1に属するプログラムが実行されている場合を例に説明する。

【0043】まず、図8(a)に示すように、サービス別領域440-2のディレクトリ1に属するプログラム(図中、反転表示)が実行されている間に、ホスト端末からのコマンドによりサービスnが指定されても、つまり、サービス別領域440-0内のルートディレクトリにカレントが設定されても(ステップS201:Yes)、制御部300は、セキュリティプログラムの動作に基づいて、このカレントが設定されたルートディレクトリ(さらなるディレクトリが存在する場合は、指定されたディレクトリ)に属するプログラムの実行を許可しない(ステップS202)。

【0044】一方、図8(b)に示すように、現在実行しているサービス2のプログラム(図中、反転表示)が、サービス別領域440-1のプログラムの実行を要求した場合(ステップS203:Yes、S204:Yes)、制御部300は、セキュリティプログラムの動作に基づいて、要求されたプログラム(図中、サービス別領域440-1内、ルートディレクトリ直下のプログラム)の実行を許可しない(ステップS205)。また、この場合、例えば実行中のサービス2のプログラムが、サービス別領域440-1内のデータファイルからデータの取得を要求しても、制御部300はこれを許可しない。

【0045】しかし、実行中のサービス2のプログラムが、サービス別領域440-2のディレクトリ2に属するプログラム(不図示)の実行やデータファイル(不図示)からデータの取得を要求した場合(ステップS203:Yes、S204:No)は、HWWFが設定されているサービス別領域440-2内であるのでこれを許

可する(ステップS206)。

【0046】アプリケーションプログラム実行中は、制御部300がステップS201~S206の処理を常に行い、アプリケーションプログラムの動作を監視する(ステップS207:No)。

【0047】当該アプリケーションプログラムの実行が終了すると(ステップS207:Yes)、制御部300は、カレントディレクトリを、サービス別領域440-2のディレクトリ1からMFディレクトリに変更設定する(ステップS208)。

【0048】ステップS208でMFディレクトリがカレントディレクトリとなったことを契機に、制御部300は、セキュリティプログラムの動作に基づいて、サービス別領域440-2に設定していたHWWFを解除して(ステップS209)、図4に示すプログラム実行処理に戻り、処理を終了する。

【0049】以上説明したように、本発明にかかる実施の形態によれば、複数のサービスを実現するICカード100で実行されるプログラムに対して、サービス指定時に動的にHWWFを設定するので、予め監視対象のメモリ領域を設定することでHWWFを固定的に設定する場合と異なり、DF領域240へのプログラム(アプリケーションプログラム)やデータの追加・更新により自由度を持たせることができ、複数種類のプログラムを記録することで複数種類のサービスの利用を実現するICカードの利便性を有効に活用することができる。

【0050】また、本実施の形態で設定されるHWWFは、あるプログラムが実行されている間に他のサービスが指定されることを禁止するとともに、実行されているプログラムが他のサービスのプログラム(他のサービス別領域440に記録されているプログラム)を実行することを禁止するので、不正なプログラムを記録・実行することによる不正動作を防止することができる。

【0051】上記実施の形態では、本発明をCPU(制御部300)を実装するICカード100に適用した例を説明したが、本発明が適用可能な記録媒体はこれに限られない。例えば、CPUを実装しないICカード(メモリカード)に記録された複数のプログラムをホスト端末が実行する形態に本発明を適用してもよい。さらにこの場合、ホスト端末は専用装置に限られず、例えばパーソナルコンピュータなどの通常のコンピュータシステムを利用してよい。この場合、上述の処理を実現するプログラムをコンピュータにインストールして実行することで、上述の制御部300の動作と同様の動作を実現することができる。

【0052】ここで、コンピュータにプログラムを供給する方法は任意である。例えば、上記プログラムを記録した媒体(例えば、フレキシブルディスク、CD-ROM (Compact Disc Read-Only Memory)、DVD (Digital

1 Versatile Disk)などからインストールしてもよく、または、例えば通信回線、通信ネットワーク、通信システムなどを介して供給してもよい。この場合、例えば、通信ネットワークの掲示板(BBS: Bulletin Board System)に当該プログラムを掲示し、これをネットワークを介して搬送波に重畳してコンピュータに配信する。そして、このプログラムを起動し、OSの制御下で、他のアプリケーションプログラムと同様に実行することで、上述の処理を実行することができる。

【0053】

【発明の効果】以上説明したように、本発明によれば、プログラム実行時の安全性を効果的に確立することができるプログラム制御装置および方法、ならびにプログラムを提供することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態にかかるICカードの外観と、ICカードのICチップ内の構成を説明するための図である。

【図2】図1に示すDF領域部の詳細を説明するための図である。

【図3】図1に示すMF部とDF領域部との関係を説明するための図である。

【図4】本発明の実施の形態にかかるプログラム実行処理を説明するためのフローチャートである。

【図5】図4に示す処理の例を説明するための図であ

り、(a)は共通プログラムの実行時の処理を説明するための図であり、(b)は、所定のサービスのルートディレクトリが指定された場合の処理を説明するための図である。

【図6】図4に示す処理の他の例を説明するための図であり、(a)は他のサービスのルートディレクトリが指定された場合の処理を説明するための図であり、(b)は、サービス別領域内のディレクトリが指定された場合の処理を説明するための図である。

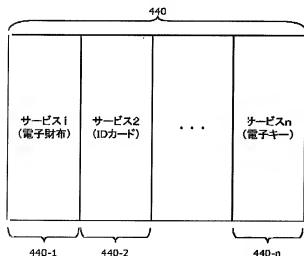
【図7】図4に示すHWWFによる監視処理を説明するためのフローチャートである。

【図8】図7に示す処理の例を説明するための図であり、(a)はプログラム実行時に他のサービスが指定された場合の処理を説明するための図であり、(b)は実行中のプログラムが、他のサービスのプログラムやデータを指定した場合の処理を説明するための図である。

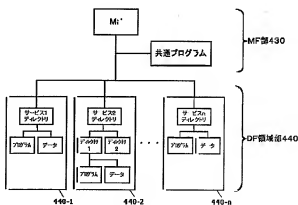
【符号の説明】

- 100 ICカード
- 200 ICチップ
- 300 制御部
- 400 メモリ部
- 410 作業領域部
- 420 OS (Operation System) 部
- 430 MF (Master File) 部
- 440 DF (Dedicated File) 領域部

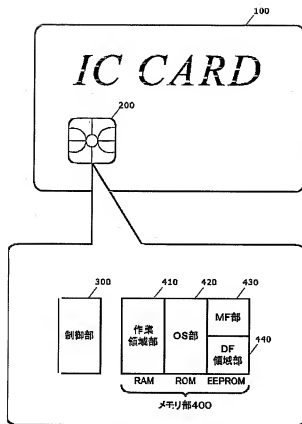
【図2】



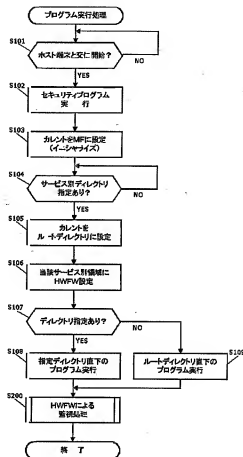
【図3】



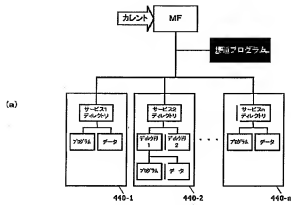
【図1】



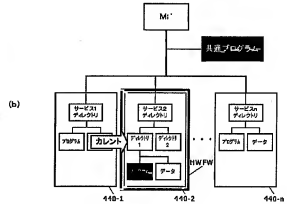
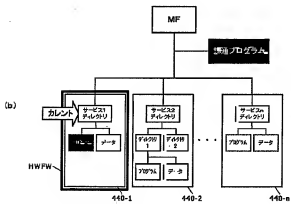
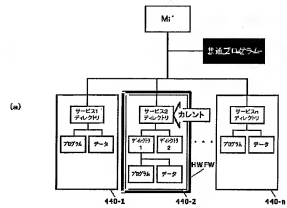
【図4】



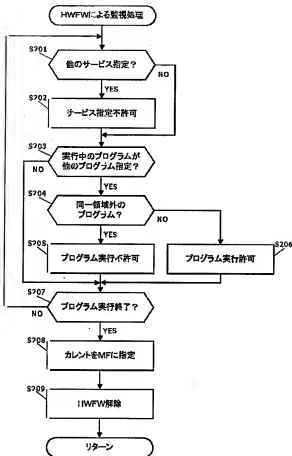
【図5】



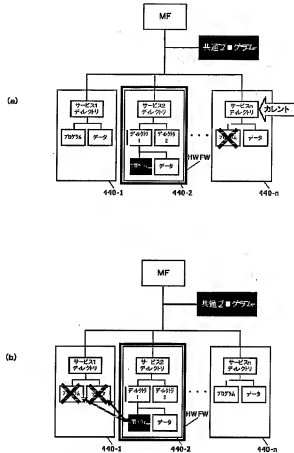
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 市原 尚久
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内

(72)発明者 山本 真也
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内
Fターム(参考) 2C005 MA01 MB05 SA22 SA25
5B035 AA13 BB09 CA11 CA38
5B076 FB01 FB02 FB03